2018 年 2 月

株式会社ワイドテック

IT システム構成管理を自動化・可視化し、脆弱性問題に備える

はじめに

昨年発見され、今年に入りメディアで大きく報道された「Meltdown」と「Spectre」という、プロセッサ・チップの脆弱性が深刻な問題になっている。
この脆弱性はチップにとどまらず、OS やアプリケーションにも影響が及ぶことも相まって、システム運用管理者にとって非常に複雑な問題と認識されている。そのうえ、関係するベンダー各社からは、対応情報や修正アップデートが五月雨式に発表されるため、対応はもぐらたたき的にならざるを得ない。このため、システム運用管理者は日々対策に追われることになり、息つく暇がない。

このような問題に迅速に対処するためには、OS やそのバージョン、修正アップデートの状況、設定内容などの IT システム機器の構成情報をこまめに収集し、予防措置を講じ、問題が生じた際は対象を特定してリスクを早めに把握できることが望ましい。
しかしながら、システム運用管理者は、ユーザーからの依頼や障害対応など日々の業務に追われ、構成情報の管理に時間を割く余裕は多くはない。また、最近増えている「1 人情シス」と言われる、1 人で社内の IT システム全般を管理しているような体制のスタートアップ企業や小企業でも、対応は難しいだろう。

しかし、今回の「Meltdown」や「Spectre」に匹敵するレベルの深刻な脆弱性を持ち、緊急度、重要度ともに高いセキュリティ事案が発生する可能性は今後も大きく、今回の経験を踏まえて事前に対策を検討しておく必要があるだろう。
そうした対策に威力を発揮するのが、IT システムの見える化と、修正アップデートの適用や設定の一括変更を行う「構成管理の自動化ソリューション」である。ここでは、構成管理の自動化ソリューション「POLESTAR Automation」を利用した構成管理の実例や効果、そして実際に脆弱性対策に適用する場合の利用方法について考えてみたい。

本ホワイトペーパーでは、以下のような流れで構成管理の自動化の必要性と効果を説明する。

- 企業では、突発する脆弱性への対応に手を焼いている
- システム運用管理部門へのプレッシャーが高まっている
- しかし、システム運用部門の置かれる環境は年々厳しくなっている
- 見える化と標準化、そして自動化で不測の事態に備える
- POLESTAR Automation で構成情報の管理やファイル適用の自動化を行う
- POLESTAR Automation を「Meltdown」と「Spectre」対策に活用する
- 定型作業の自動化により、少ない人数で脆弱性対策を迅速かつ確実に行う

企業では、突発する脆弱性への対応に手を焼いている

昨年、「Meltdown」と「Spectre」という、プロセッサ・チップで見つかった 2 つの脆弱性が、今、企業のシステム運用管理部門で大きな問題になっている。この脆弱性への対処に手を焼いているのは、プロセッサだけでなく、ハードウェアやソフトウェアベンダーなど複数の関係者が絡み合っているためである。
この問題を解決するためには、該当するプロセッサを搭載するハードウェアを交換するのが最も簡単ではあるが、費用的な面を考えれば、現実的ではない。したがって、既存のサーバーやネットワーク機器を安全に有効活用するため、ハードウェア、OS やアプリケーションなど、幅広い分野での修正アップデートの適用などの対策が必要になる。
現在、US-CERT（米国国土安全保障省配下の情報セキュリティ対策組織）では、「Meltdown」と「Spectre」の対策として、各ベンダーの指示に従うことを推奨しており、現在 40 社以上のベンダーやプロジェクトのセキュリティ・サイトへのリンクが掲載され、参照を促している [(1)]（2018 年 1 月 25 日現在）。
また、さらに悪いことに、修正アップデートを適用することで、CPU のパフォーマンスが落ちるという事例が発表されている。この問題を改善するため、続々リリースされる修正アップデートをいちいち適用したり、一度リリースされた修正アップデートをアンインストールしたりと、何度も何度も対策を講じなければならなくなる場合がある。

一昨年にも「Wannacry」と呼ばれる重大な脆弱性事案があり、システム運用管理者の迅速な対応が必要とされ、担当者が右往左往する場面があった。
この手の脆弱性の問題はネット上で一気に拡散し、多くの人が知ることになるため、対策を施さないことによるリスクは日に日に高まる。よって、素早い対策が求められるのである。
システム運用管理部門では、今、鬱積する「Meltdown」と「Spectre」問題への対応に頭を悩ませている。

システム運用管理部門へのプレッシャーが高まっている

このように、脆弱性の問題は突然発生し、一挙にリスクが高まる。脆弱性を突こうとするハッカーは、対応を待ってくれるわけではない。このため、何らかの脆弱性の問題が発表されると、社内的にその影響範囲の特定と対策の素早い実施が求められ、システム運用管理部門にプレッシャーとして重くのしかかってくる。
もし、IT に詳しい企業のトップであれば、脆弱性の問題が発覚した時に、次のように IT 部門長に確認するかもしれない。「当社のサーバーはこの脆弱性への攻撃を受けても大丈夫か？どんなリスクが考えられるのか？」と。
そのとき、IT 部門長は、即座に自社における脆弱性の影響範囲と、対策スケジュールを答えることができるだろうか。保有しているサーバーやネットワーク機器の OS や修正アップデートの適用情報などの最新構成情報を持っていないと、即座にとは言わないまでも、一両日中にその回答を行うことは難しいだろう。

実際には、各サーバーやネットワーク機器にアクセスし、必要な情報を収集し、Excel に転記しまとめるというような作業を、迅速に行わなくてはならない。機器の台数が少なければよいが、300 台、500 台、1000 台とな

ると、気が遠くなることだろう。調査だけで数週間から 1 か月以上もかかってしまうかもしれない。そうなると、対策はどんどん後手に回ることになる。
ある企業では、「Wannacry」の脆弱性問題発覚時に、対象範囲を特定しようとして 300 台のサーバーの情報を収集するために 3 週間を要したという話がある。
具体的な対応は次のようになるだろう。サーバーの CPU や OS の種類、バージョン、修正アップデートの適用状況、ロケーションなど、関係する情報を収集する一方で、ベンダーから修正アップデートを収集し、影響の度合いやリスクを勘案したうえで、事前に検証を行う。そして、修正作業のための方針と戦略を決め、それを実行する。これらを短期間で実施しなければならない。

IT システムが複雑かつ大掛かりになるにつれ、脆弱性に伴う影響度も拡大する。システム運用管理部門に求められるプレッシャーは、今後も強まり続けることだろう。

しかし、システム運用管理部門の置かれる環境は年々厳しくなっている

しかしながら、システム運用管理部門の業務は、脆弱性への対策だけではない。ユーザー部門からの日々の要望に応えるための作業や障害対応、パフォーマンスの改善など、さまざまな業務をこなさなければならない。
多くのビジネスがシステム化され、システム運用管理部門が対応しなくてはならないシステムは、年々増加している。そして、仮想化やクラウド、モバイルといった技術が日々進歩することで、企業の IT システム環境はますます複雑さを増している。例えば、物理・仮想の混在、データセンターや複数のクラウドサービスに配置したさまざまなサーバーの管理といった、ハイブリッドな環境の管理も増えている。
そのうえで、ビジネスにおける IT システムの重要性が増すのにともない、より高いサービス品質と運用品質が求められることになる。
図 1 にシステム運用管理部門が置かれている厳しい環境を示す。

一方で、現在の人材市場においてスキルを持つ IT エンジニアを必要数確保することは、非常に難しい状況になっている。経営チームからの TCO 削減の要求もあるため、人員を増やすことは容易ではない。
このように、システム運用管理者の置かれている環境は、年々厳しくなってきている。

図 1　システム運用管理部門が置かれている環境

見える化と標準化、そして自動化で不測の事態に備える

突然顕在化する脆弱性事案への迅速な対応や、IT システムの健全性を日々確認するために、システムの構成情報の管理は必須となる。サーバーやネットワーク機器の構成情報を毎日収集し、システム運用管理基準等のポリシーに照らし合わせて点検し、問題をタイムリーに確認できるようにする。
そして、チェックする内容や手順を決めておく。さらに、修正アップデートの適用や設定の変更における事前検証の方法や承認フローを定義しておく。構成情報の見える化と標準化を行うことで、突発的な脆弱性事案の顕在化にも、慌てず騒がず対応しやすくなる。

サーバーやネットワーク機器の構成情報を確認するためには、各機器にアクセスし、最新のステータスを収集しなければならない。それも、定期的かつ頻繁に実施しなければ、日々変更されるシステムの構成情報を把握できない。サーバーやネットワーク機器の数が増えれば増えるほど、定型作業が増えていくことになる。
ある調査では、システム運用管理の作業において、毎日または毎週など、周期的に繰り返して実行する必要のある作業は、全体の 45%程度あると言われている[(2)]。これらの周期的、定型的な作業は、自動化ソリューションに代行させやすい。そして、対象となる機器の数が増えれば増えるほど、自動化ソリューションによる省力化の効果が見込める。
修正アップデートの適用や、ログイン・パスワードの文字数設定といったポリシーの一括変更なども、自動化が効果を発揮する作業である。

また、障害原因の 65%以上を占めるのが人的ミスと言われており[(3)]、IT サービスの品質はシステム運用管理者のレベルによって大きく左右されることが知られている。作業を標準化し、かつ自動化することで、人的ミスの撲滅が実現できる。具体的には、作業の手順やノウハウをスクリプトに記述することで標準化を図っておけば、

作業はそれを実行するだけで、ミスなく自動的に完了できるようになる。
こうした標準化・自動化により、少ない人数で多くの作業をこなせるようになるだけでなく、人的ミスも防止できる。

脆弱性の問題が突然発覚した場合は、構成管理情報で対象となる機器や OS を特定し、検証を終えた修正アップデートや設定を自動的に一括適用できるようにしておくことで、リスクに素早く対処できる。
表 1 は、ある企業において、自動化ソリューションの導入により達成された省力化の実績である。

表 1　自動化ソリューション導入による省力化効果（サーバーが 3,000 台規模）

内容	導入前	導入後	改善率
Windows 導入済みソフトウェア一覧の検索	197 時間	4 時間	**98%削減**
AIX Bug 修正パッチ適用対象サーバーの調査および情報の突き合わせ	17 時間	4 時間	**75%削減**
Crontab 登録スクリプトエラーチェック時間	57 時間	14 時間	**75%削減**
サーバー全アカウントのパスワード一括変更	7.4 時間	0.4 時間	**95%削減**
サーバー構成管理基本情報の突き合わせ	199 時間	0.2 時間	**99%削減**

POLESTAR Automation で構成情報の管理やファイル適用の自動化を行う

POLESTAR Automation は、サーバーの構成管理、バッチジョブ実施、監査、配布、設定変更、システム/セキュリティ点検などのシステム運用管理業務の多くを自動化するアプリケーションである。
脆弱性対策という観点から POLESTAR Automation の特長をまとめると、次の 3 点になる。

- サーバーやネットワーク機器、仮想化環境の OS バージョンやパッチの適用状態、そして設定内容などの情報を自動的に収集。そして、管理下にある機器の情報を一元的に表示できる。
- あらかじめ策定しておいた管理ポリシーを基準に、それと比較しての順守状況、違反状況を確認できる。
- さらに、OS のバージョンアップや修正アップデートの適用、設定変更を自動的に実行できる。

加えて、構成情報を定期的に取得しておくことで、時系列での構成情報の変化を確認できるスナップショット機能や、リモート機器に都度アクセスして設定状況の確認や変更ができるアドホック・コマンド機能などが利用できる。

さらに、POLESTAR Automation にはこれまでシステム運用管理者が行ってきた、実施頻度の高い作業手順やノウハウのベスト・プラクティスを組み込んだ標準ジョブテンプレートが付属している。このため、このテンプレートを活用し、自社にあった内容に修正することで、導入後すぐに構成管理の自動化を実現できる。
図 2 に POLESTAR Automation の 6 つの特長を示す。赤文字は、特にシステム運用管理者が実際の運

用にあたり、多くの恩恵を得られるものである。次に何をすればよいのか、マニュアルを読まなくても理解できる直観的なユーザビリティ、標準ジョブテンプレートの豊富さ、そして Windows、Linux、商用 UNIX、ネットワーク機器、仮想化環などを一括で管理できるプラットフォームとしての機能など、魅力的な機能が備わっている。
図３、図４は構成情報の出力例を示している。

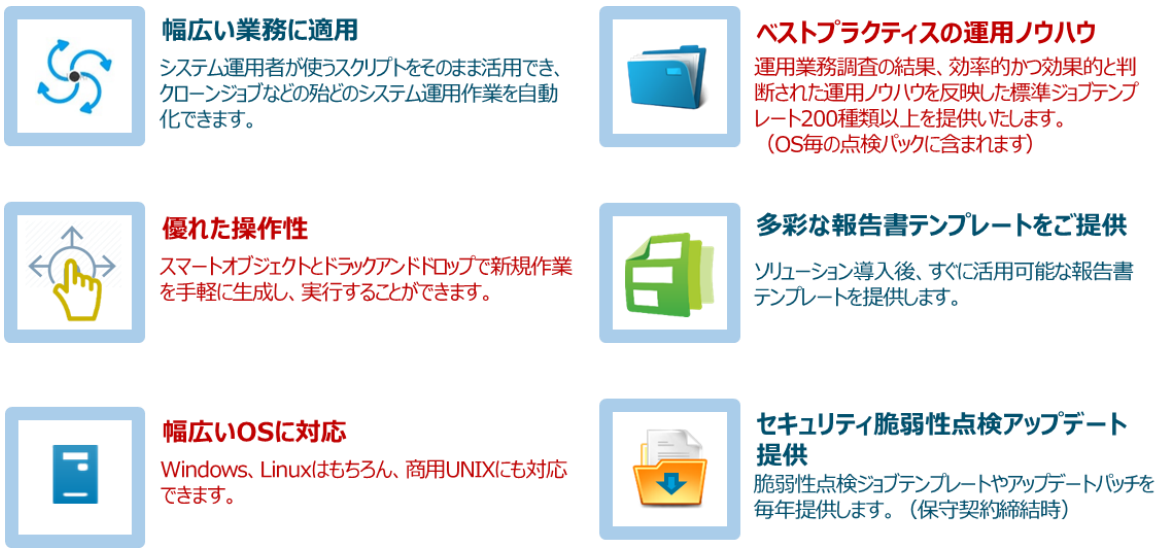

図２　POLESTAR Automation の特長

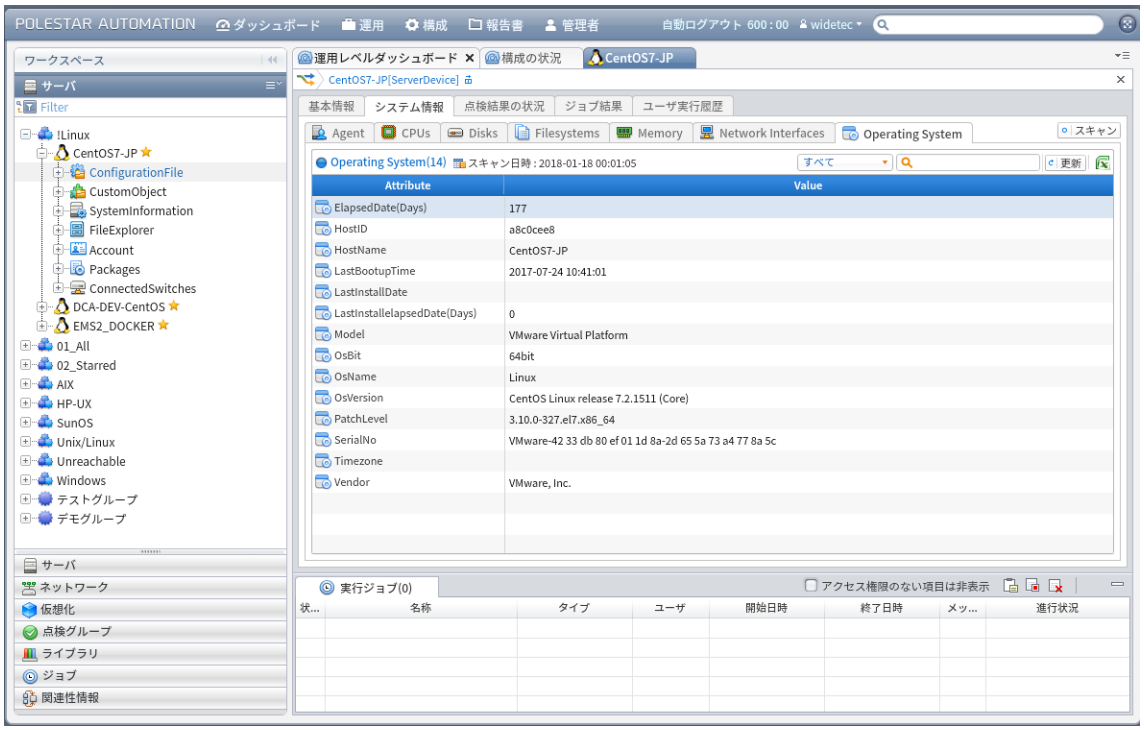

図３　サーバー情報（CentOS サーバーの OS 情報）の表示例

サーバ構成情報

サーバ名	シリアル	IP	筐体	CPUモデル	CPUクロック	Physical Core	Logical Core	メモリサイズ	ディスクサイズ	全体NIC数	NICタイプ	使用中のNIC数	OS種類	OS名称	OSパッチレベル	OSカーネルビット	ElapsedDate (Days)	LastBootup Time	Persisted Date
rx2800i1	SGH501Y32W	192.168.200.103	ia64 hp Integrity rx2800 i4	Intel(R) Itanium(R) Processor 9550 (2.39 GHz, 32 MB)	2390	4	4	66968332	1555	1	1000000	1	HP-UX	HP-UX	1403	64bit	203	2018-12-12 09:17:28	2017-07-03 21:57:18
DB-QA	VMware-42 2a 91 a7 f9 f9 4f c0-33 1a 03 80 3d df 3a d4	192.168.202.48	VMware Virtual Platform	Intel(R) Xeon(R) CPU E5-2696 v3 @ 2.30GHz	2300	8	8	16778628	153	1	10000000	1	Windows	Microsoft Windows Server 2008 R2 Enterprise	Service Pack 1	64bit	39	2017-12-14 03:18:44	2019-01-22 10:30:01
solaris11		192.168.202.49	VMware Virtual Platform	x86	2600	2	2	4193932	53	1	1000000	1	SunOS	SunOS		64bit	218	2018-11-29 08:13:12	2017-07-03 21:57:31
WIN2012R2DEV	VMware-42 33 9b 18 18 e0 a4 6a-fc 98 80 19 39 3a e1 14	192.168.202.52	VMware Virtual Platform	Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz	2600	10	10	25165384	204	1	10000000	1	Windows	Microsoft Windows Server 2012 R2 Datacenter		64bit	78	2017-11-07 10:03:13	2019-01-22 10:30:24
CentOS7-JP	VMware-42 33 cb 80 af 01 1d 8a-2d 85 3a f3 a4 77 8a 5c	192.168.202.208	VMware Virtual Platform	Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz	2600		1	1884512	0	1	10000000	1	Linux	Linux	3.10.0-327.el7.x86_64	64bit	184	2017-07-24 10:41:00	2019-01-23 00:01:05
EMS2_DOCKER	VMware-42 33 d5 69 42 f0 99 a9-90 3a df 02 8a b3 4a 0d	192.168.202.34	VMware Virtual Platform	Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz	2600		2	3883016	0	1	10000000	1	Linux	Linux	3.10.0-229.14.1.el7.x86_64	64bit	486	2018-10-13 11:36:01	2019-01-23 00:01:05
DCA-DEV-CentOS	902.20X1	192.168.10.180	Inspiron 7520	Intel(R) Core(TM) i7-3632QM CPU @ 2.20GHz	2200	4	8	3794772	1000	1	100000	1	Linux	Linux	2.6.32-431.el6.x86_64	64bit	27	2017-12-28 10:28:32	2019-01-23 00:01:08
EMS3-TEST	JCY3YP1	192.168.10.62	Dell System XPS L502X	Intel(R) Core(TM) i7-2720QM CPU @ 2.20GHz	2201	4	8	9300719	610	2	100000	2	Windows	Microsoft Windows 10 Home		64bit	2	2018-01-22 18:27:08	2019-01-23 00:01:48
NIDA-PC-PC	H4H2DW1	192.168.10.85	Inspiron 3323	Intel(R) Core(TM) i5-3337U CPU @ 1.80GHz	1801	2	4	2097132	476	1	100000	1	Windows	Microsoft Windows 7 Starter K	Service Pack 1	32bit	0	2018-01-24 19:58:11	2019-01-23 00:01:31

図４　管理対象サーバーの構成情報報告書例

POLESTAR Automation を「Meltdown」と「Spectre」対策に活用する

それでは、「Meltdown」や「Spectre」対策での POLESTAR Automation の活用方法を考えてみよう。事前にサーバーやネットワーク機器の構成情報を把握しておき、同じ OS やロケーション、部門等でグルーピングしておけば、一括での確認や修正適用が容易になる。

まず、Intel から提供されている「CPU 脆弱性点検プログラム」を利用して脆弱性を点検する。
POLESTAR Automation では、点検プログラムを全サーバーに一括配布し、実際に点検するところまでの作業を、簡単に作成できる。システム運用管理者が個々のサーバーにアクセスして配布、実施する必要はない。
図５と図６に、点検プログラムの配布設定と、配布後の点検についての設定画面を示す。

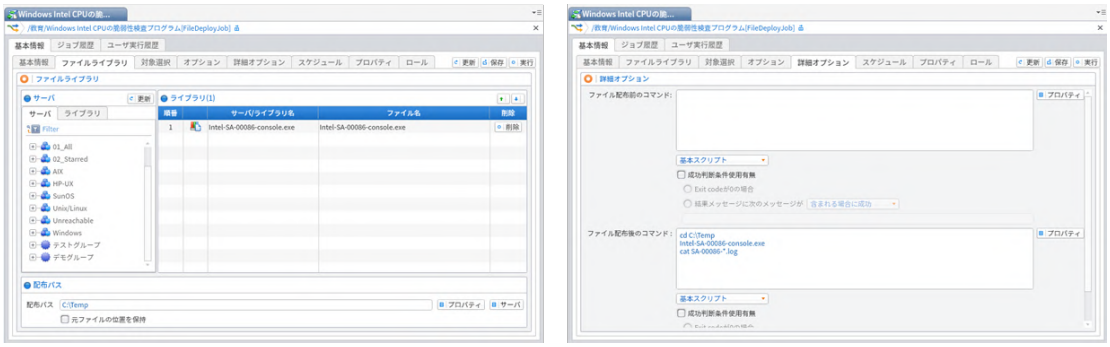

図５　プログラム配布ファイル設定画面（左）ファイル配布後点検プログラム実行設定画面（右）

図６および図７は、点検プログラム配布、実行後の点検結果ログの画面である。「Status: This system is not vulnerable.」と表示される場合、CPU の脆弱性に対するパッチは必要でなく、「Status: This system is vulnerable.」と表示される場合にはパッチが必要であると判断することができる。

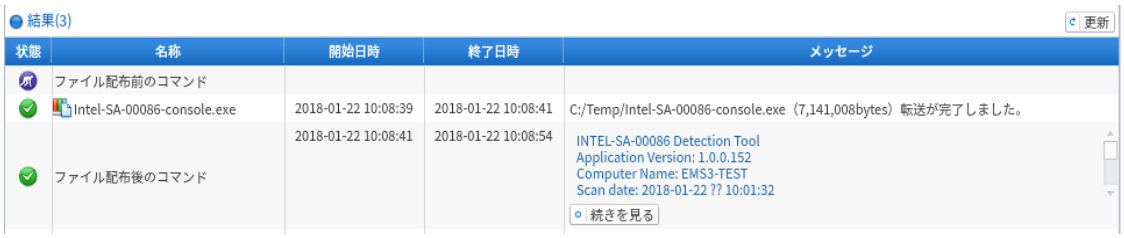

図６　点検結果ログの表示（実行結果のフラッシュ）

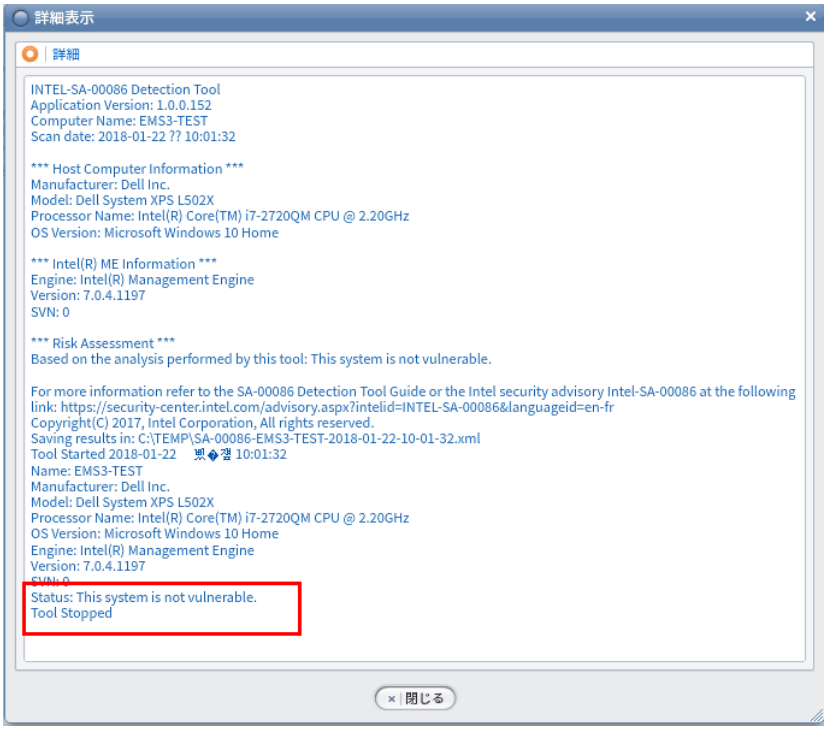

図７　点検結果ログの表示（全ログ表示）

このように、POLESTAR Automation を利用すれば、点検プログラムの配布と実施、ログ収集という一連の作業を自動化することができる。

このほか、「Meltdown」や「Spectre」対応では、以下のような定型的な作業を自動化が可能である・

- ベンダーから提供される対策用の修正アップデートの一括導入 [ファイル配布バッチジョブ機能]
- 機器ごとに、どんな修正アップデートが適用されており、何が適用されていないかの確認 [点検機能]
- 修正アップデートのアンインストール（必要に応じて）[スクリプトジョブ機能]
- 時系列での構成情報の変化の確認 [スナップショット機能）
- 全サーバー、ネットワーク機器の OS,ミドルウェア、アプリ、CPU、ディスク等の構成情報を日々収集することで、健康状態をチェック [構成情報収集機能]

また、これまでに発表された、そして今後発表される OS やアプリケーション・ベンダーから発表されるさまざまな修正アップデート対応も必要となる。一度適用した修正アップデートのアンインストールが必要になるかもしれない。このような場合でも、POLESTAR Automation であれば、ジョブテンプレートを作成し、グループ化されたサーバーやネットワーク機器に一括適用することができる。

定型作業の自動化によって、より少ない人数で脆弱性対策を迅速かつ確実に行う

システム運用管理者は、大型化し益々複雑になるシステムや、絶え間ないテクノロジーの進化に合わせ、システムのサービスレベルや運用レベルを少しでも高めるべく、日々努力していることであろう。
しかし、脆弱性の問題や障害の対応などでは、社内からの大きなプレッシャーを受け、時間との戦いを強いられる。人員の確保も容易ではなく、少ない人数で厳しい状況をしのがざるを得ない状況が続いている。
サービスレベルを落とすことなく、このような状況に対処するには、定型業務の標準化を行い、それらを極力自動化していくことが必須になっていくだろう。
少人数で突発的な問題に迅速に対応するためには、構成管理の自動化ソリューションである POLESTAR Automation が、強力な武器になる。

そして、システム運用管理者が試行錯誤を重ねながら獲得してきた、ミスを減らすための運用ノウハウや手順。その経験から得られた知見を標準化することで、高度な運用ノウハウや手順が蓄積される。その結果、運用管理業務の完成度を高めていくことができる。
POLESTAR Automation のような自動化ツールの活用により、運用管理業務に必要な時間を確保し、予防手段を講じることで、障害の原因を事前に排除することができる。

時間という限界がある。
定型的な作業を極力自動化し、今後生まれるだろうビジネスやテクノロジーの変化に追従していくための時間を確保できなければ、明日はない。

(1), https://www.us-cert.gov/ncas/alerts/TA18-004A
(2) (3) 2016 年 NKIA 社調査結果

本件に関するお問い合わせは下記 POLESTAR 営業担当までお願いします。

株式会社ワイドテック
プロダクト事業部 POLESTAR 営業担当　　e メール：POLESTAR@widetec.com
〒101-0032 東京都千代田区岩本町 2-11-2 イトーピア岩本町 2 丁目ビル
電話：03-5829-4178
製品 HP: https://polestar.widetec.com
会社 HP：http://www.widetec.com